

S- 91,131

IL-10,360

SYSTEM AND METHOD FOR
MULTIMEDIA ENCRYPTION

BY

Douglas R. Coffland (USA)
5674 Wisteria Way
Livermore, CA 94550

Patented Feb 23, 1994

1 SYSTEM AND METHOD FOR MULTIMEDIA ENCRYPTION

2

3 The United States Government has rights in this invention pursuant
4 to Contract No. W-7405-ENG-48 between the United States Department of
5 Energy and the University of California for the operation of Lawrence
6 Livermore National Laboratory.

7

8 BACKGROUND OF THE INVENTION

9 1. Field of the Invention

10 The present invention relates generally to systems and methods for
11 encryption, and more particularly for multimedia encryption.

12 2. Discussion of Background Art

13 Transmission of audio and video signals, such as video conferencing
14 and security surveillance signal, across both local and wide area networks is
15 becoming more and more commonplace in today's globally interconnected
16 internet driven economy. In such applications, encryption is often required
17 for protecting and authenticating such multimedia signals as they travel over
18 unsecured networks. For instance, corporations often exchange business
19 sensitive information during such conferences which must not be
20 intercepted. Additionally, multimedia information from networked security
21 camera systems must be authenticated and protected from unauthorized
22 monitoring.

1 A degree to which encryption authenticates and protects multimedia
 2 data depends on the encryption schema used, an encryption key length, the
 3 predictability of the encryption key, and how the encryption keys are
 4 protected. Typically, encryption keys are generated by hashing algorithms
 5 from random number seeds provided by a source which hopefully provides
 6 random number seeds. Random number seeds, however, are extremely
 7 difficult if not impossible to generate using algorithmic methods on digital
 8 computers, since algorithms executing on digital computers are by nature
 9 deterministic. As a result, various external chaotic sources have been used to
 10 generate the random number seeds.

11 Examples include methods described in U.S. Patent 5,732,138 entitled,
 12 “Method For Seeding A Pseudorandom Number Generator With A
 13 Cryptographic Hash Of A Digitization Of A Chaotic System,” by Noll et al.,
 14 and U.S. Patent 5,774, 549 entitled, “Method And Apparatus That Processes A
 15 Video Signal To Generate A Random Number Generator Seed” by Jakob
 16 Nielsen.

17 Noll discusses generating seeds by applying a hashing algorithm to a
 18 digitized chaotic system. Chaotic systems mentioned include clouds moving
 19 in the sky, ocean waves crashing on a shoreline, and nodules moving within
 20 a “lava-lamp.” A weakness of the Noll system, however, is that in his
 21 preferred embodiment, new seed generation depends upon using dedicated
 22 input devices to monitor “real-world scenes,” such as a video camera

1 monitoring a lava-lamp, in order to obtain the necessary chaotic input for
2 eventual random number generation.

3 Nielsen also requires dedicated input devices, such as a video camera.

4 Nielsen monitors "live" scenes with a video camera and then generates
5 seeds from pixel changes within sequential frames of video data. A weakness
6 of the Nielsen system is that new seeds are not generated when motion
7 within a monitored scene stops.

8 In response to the concerns discussed above, what is needed is a system
9 and method for multimedia encryption that overcomes the problems of the
10 prior art.

a

[illegible][illegible][illegible][illegible]

1 securely transmitting multimedia data over digital networks, obtaining
2 random numbers directly from the multimedia data would be very useful.
3 These and other aspects of the invention will be recognized by those
4 skilled in the art upon review of the detailed description, drawings, and
5 claims set forth below.

SECRET

a

BRIEF DESCRIPTION OF THE DRAWINGS

1
2 Figure 1 is a block diagram of a system for multimedia encryption
3 according to the present invention;

4 Figure 2 is a graphical depiction of quantization processes within an
5 analog-to-digital converter within the system;

6 Figure 3 is a block diagram of a computer within the system;

7 Figure 4 is a graphical depiction of how a data acquisition module
8 operates within the system; and

9 Figure 5 is a flowchart of a method for multimedia encryption.

9

1 DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

2 Figure 1 is a block diagram of a system 100 for multimedia encryption
3 according to the present invention. Within the system 100, a transducer 102,
4 such as a video camera, a radio, a microphone, a Geiger counter, or an
5 electrical component, outputs a media signal 104.

6 The media signal 104 may or may not contain useful information, such
7 as an actual video scene or audio output, and the present invention does not
8 require that useful information be present. For example, while a video
9 camera could be capturing a scene, this is not required, and instead a lens-cap
10 could be on the camera causing the scene to be perfectly quiescent. In one
11 embodiment of the present invention, the media signal need only include
12 random transducer noise having a noise signal amplitude. Random noise is
13 not the same as a chaotic noise. Random noise, such as white Gaussian noise, is
14 completely unpredictable from one moment to a next, while chaotic noise is
15 highly predictable over short time periods. In a second embodiment of the
16 invention, however, random transducer noise need not even be present.
17 Instead, data compression techniques provide a basis for multimedia
18 encryption, as will be elaborated upon below.

19 The media signal 104 from the transducer 102 is fed into an analog-to-
20 digital (A/D) converter 106. The converter 106 quantizes the media signal
21 with a quantization step size smaller than the noise signal amplitude within
22 the media signal 104, creating a quantized media signal 108. The quantized
23 media signal 108 is then routed to a computer 110.

1

2 Figure 2 is a graphical depiction of quantization processes within the
3 analog-to-digital converter 106 within the system 100. The media signal 104 is
4 periodically sampled 202. The samples 202 are then quantized at predefined
5 steps 204 resulting in the quantized media signal 108. The quantized media
6 signal 108 is a quantized approximation of the media signal 104 containing
7 random transducer noise. The random noise in the media signal 104 will
8 cause even unchanging video scenes to have quantization values 206 which
9 fluctuate for media signal values close to one or more quantization steps 204.
10 Thus, even a perfectly quiescent media signal 104 (e.g. when a lens cap is on a
11 video camera containing the transducer 102) will contain some randomness
12 from random transducer noise. Put another way, as long as a size of a
13 smallest quantizer step is no larger than an amplitude of the transducer 102
14 noise, the quantized media signal 108 will include a high level of randomness
15 even if input to the transducer is perfectly quiescent.

16 Typically, the transducer noise is sufficient to cause the quantization
17 values 206 to fluctuate. However, if the transducer noise is small relative to
18 the quantization steps 204, then either video or audio content of the media
19 signal 104 must vary somewhat so that what little noise is in the scene will
20 enable random noise to be quantized by the A/D converter 106. Randomness
21 will be present in the media signal 104 when an actual sampled media signal
22 value 208 is very close to a quantization boundary 210. When this occurs, a
23 small transducer 102 signal will randomly cause the quantized media signal

1 108 to vary. It is possible to test whether sufficient random noise is present
2 within the media signal 104 by looking at least significant bits of the media
3 signal 104 and ensuring that no long sequences of a single bit value (i.e. ones
4 or zeros) exist. Long sequences of zeros or ones in a least significant bit of the
5 media signal 104 would suggest that the random noise is not of a sufficient
6 amplitude to create random numbers.

7 In an alternate embodiment, distortion may be introduced into the
8 media signal 104 generated by the transducer 102 such that the random
9 transducer noise will have an amplitude greater than the quantization steps
10 204. Distortion may be introduced, for example, in a video camera by turning
11 on an automatic gain control and increasing video camera gain. In another
12 embodiment, focus and zoom of the camera can be varied while capturing
13 video data.

14
15 Figure 3 is a block diagram 300 of the computer 110 within the system
16 100. Within the computer 110, a data compression module 302 compresses the
17 quantized media signal 108 into a compressed data stream 303 using any
18 number of formats, such as MJPEG, MPEG1, MPEG2, MPEG4, or H.261. Many
19 other standard, as well as proprietary, media compression schemes also exist
20 that are compatible with the present invention.

21 The compressed data stream 303 is partitioned into data frames of
22 varying length, depending upon an amount of information contained in the
23 media signal 104, variations in a scene or audio captured by the transducer

1 102, transducer noise, and system noise. For example, a 16384 byte amount of
2 data acquired from an MPEG1 compressed data stream can include between
3 one and eight frames of media data of varied length. For comparison,
4 uncompressed media signals generally have a frame length which is fixed in
5 size. For instance, uncompressed digital video signals include a series of fixed
6 sized digital video images.

7 Under some compression schemas, the compressed data stream 303
8 includes predictive data frames. Predictive data frames only contain
9 information which reports on differences between a current data frame and a
10 most recent full data frame. Predictive data frames typically include motion
11 vectors and error codes. Identical motion vectors and error codes between
12 full frames indicate an absence of any video motion, audio, or transducer
13 noise.

14 The compressed data stream 303 also can include compression
15 transform coefficients, frame sequence numbers, and cyclic redundancy
16 checks which vary from frame to frame. Identical transform coefficients
17 between full frames indicate an absence of any video motion, audio, or
18 transducer noise.

19 In response to a key request 304 received from an external source (not
20 shown), a control module 306 instructs a data acquisition module 308 to
21 collect a set of data 309 from the compressed data stream 303. The data
22 acquisition module 308 operating in conjunction with the data compression
23 module 302 creates a robust source of random numbers in the set of data 309.

1 This is due to unpredictable variability between the compressed data stream
2 303 and random selection of the set of data 309 therefrom.

3 In an alternate embodiment, the data acquisition module 308 can be
4 instructed to collect the set of data 309 directly from the quantized media
5 signal 108 output by the A/D converter 106 before any data compression. An
6 amount of data collected is dependent upon an amount of uncertainty
7 required for a given application. A good rule of thumb is to capture an
8 amount of data greater than or equal to a compressed full frame. However,
9 when a large amount of noise is present in the media signal, a lesser amount
10 of the media signal data needs to be collected.

11 A message digest generator 310 receives and processes the set of data
12 309 with a hashing algorithm. The message digest generator 310 generates a
13 fixed-length unique identifier 311 for each pattern of bits in the set of data 309.
14 Hashing algorithms assure that the resultant identifier 311 varies significantly
15 even if the set of data 309 only varies by one bit. It is computationally
16 infeasible to reconstruct the set of data 309 from only knowledge of the
17 identifier 311. This identifier 311 is also called a keyword seed.

18 An encryption key generator 312 is a pseudo-random number
19 generator that receives and processes the identifier 311 into a set of keywords
20 to be immediately used or stored in a memory 314 for later use.

21

22 Figure 4 is a graphical depiction 400 of how the data acquisition module
23 308 operates within the system 100. Shown is a typical compressed

1 multimedia data stream 402. The data stream 402 includes compressed audio,
2 video, and control data separated by frame boundaries 404. Each frame of data
3 has a length, such as video data 406, which has a length 408. Within the
4 multimedia data stream, lengths of each frame vary randomly, depending on
5 a compression ratio as well as other well known compression algorithm
6 factors. The data acquisition module 308 acquires a set of data 410 from the
7 compressed data stream 303 without regard to any of these factors.

8 Thus, the set of data 410 can cross over the frame boundaries 404 in a
9 random manner, resulting in a highly random, and unpredictable set of data
10 309. The set of data 309 thus can function as a robust keyword seed.

11
12 Figure 5 is a flowchart 500 of a method for multimedia encryption. The
13 method begins in step 502 where the transducer 102 receives a media signal
14 which may include a noise signal amplitude. In step 504, the A/D converter
15 106 quantizes the media signal with a quantization step size smaller than the
16 noise signal amplitude. The data compression module 302 compress the
17 media signal into data frames having data frame boundaries, where the data
18 frames may have similar or varying lengths, include compression transform
19 coefficients, and/or include predictive data frames in step 506. Next, in step
20 508, the data acquisition module 308 selects a set of data from the compressed
21 media signal, such that the data selected may include one frame of data, data
22 which crosses over several data frame boundaries, compression transform
23 coefficients, and/or predictive data frames. In step 510, the message digest

